

REMARKS

The Examiner points out that the amendment filed on August 31, 2006 addresses the rejection under 35 U.S.C. § 103(a) based on the hypothetical
5 combination of Van Oorschot and Nardone, but does not specifically address the other rejections or the prior art relied on therein. Applicant herein specifically addresses each rejection and all of the prior art cited by the Examiner.

Claims 1-7, 14, 16-17, 19, 23 and 25-29 are rejected under 35 U.S.C. §
10 103(a) as being obvious in a light of a hypothetical combination of Van Oorschot and Nardone. Applicant respectfully traverses this rejection. The Examiner has now asserted patent No. 5,805,700 issued to Nardone, in combination with Van Oorschot (USPN 5,850,443), as to basis for finding the claimed invention to be obvious.

15 In this regard, Nardone indeed discloses that only a part of video data has to be encrypted in contrast to encrypting the entire content. As outlined in Nardone at column 1, line 28 and column 1, lines 45-50, the partial encryption of basis transfer units of compressed video data of video images helps to reduce processing requirements.

20 However, Nardone is completely silent on the specific key management as defined in Claim 1. If at all, Nardone only discloses the third paragraph of Claim 1, stating that the second section of the payload data remains unencrypted. Regarding the kind of encryption, please refer to column 2, line 67 of Van Oorschot, where a "stream cipher technique" is mentioned. A key for

this symmetric cipher has to come from somewhere, so Nardone possibly suggests the features of the second paragraph of Claim 1.

However, Nardone is completely silent on the steps of processing, linking, encrypting, and entering. Therefore, from a claim having six steps,
5 Nardone only discloses two steps.

To summarize, Nardone discloses to encrypt only a part of a video sequence using a stream cipher (column 2, line 65). All this is done to obtain a similar level of encryption because the video images are degraded to a virtually useless state. Furthermore, processing power is saved, as outlined in column
10 1, lines 47 to 50.

However, Nardone is not at all interested in protection of the unencrypted sections. Nardone does not teach or suggest to do anything in that direction. Instead, Nardone teaches completely away from the claimed invention because the claimed invention incurs additional processing steps, introducing additional
15 delay, and acquiring additional computational resources by performing the last four steps of Claim 1, which is against the teaching of Nardone, which says that one only has to encrypt the part of data to save processing power.

Thus, why should those skilled in the art go against the teaching of Nardone and introduce any additional protection features for the non-encrypted
20 part of the useful data. In view of that, Nardone cannot render obvious the subject matter of the claimed invention.

Applicant will discuss Van Oorschot in more detail. Importantly, Van Oorschot has, as outlined in the first paragraph of column 3, two scenarios. The first scenario is a low-trust environment. A low-trust environment means
25 that a probability exists that the cryptographic protection has to be defeated for

national security or law enforcement reasons. Stated differently, when an encrypted message comes from a low-trust environment, for example from a region which is known for terrorist activities, then the National Security Authority must have a chance to defeat the cryptographic protection, *i.e.* to decrypt the encrypted content against the will of the sender of the encrypted content.

Now, the question is, how this is achieved in Van Oorshot. As stated in connection with Fig. 3, this defeating feature is introduced by the X-fields, and the fact that the message is encrypted using a short low-trust symmetric key K' . The symmetric key K' , which is a low-trust symmetric key, is encrypted using a low-trust public key from the sender of the message. This low-trust public key, as well as the low-trust symmetric key encrypted using the low-trust public key, are written into the X-fields, as outlined in column 7, lines 5 to 7.

Now, one has to raise the question, why these fields are written into the bit stream in plain text. The answer is that the 512-bits RSA public key of A can be used for sending and for retrieving a corresponding RSA private key of A which can, for example, be performed by a Law Enforcement Authority which has received an authorization by one or more judges or other trusted agents, as indicated in column 2, lines 56-58. Then, those law enforcement agencies would decrypt the encrypted low-trust symmetric key K' using the second X-fields, which would then mean that the decryption of the encrypted message without any usage of A's header field or B's header field is required. This is important because the Law Enforcement Agency is not forced to find a private key belonging to a high-trust public key of A because the high-trust public key of A is 1024 bits long, *i.e.* has double the length of the low-trust public key, the

effort for determining the private key belonging to the public key is much higher compared to the low-trust public key, which can be defeated easier.

In this context, in normal encryption it is completely useless that the sender or originator of a message encrypts anything using his own public key
5 because the only person being in the position to decrypt this item is the sender or originator himself because he is the only person knowing his private key.

However, cryptographic systems are never unbreakable, and for example, for the Central Intelligence Agency, it is much easier to break a 512-bits private key as included in the X-fields compared to a 1024-bits private key
10 enclosed in A's header field.

Now, another question is what a straight-forward combination of Van Oorschot and Nardone would look like. Such a combination could mean that only a part of the symmetrically encrypted message would be encrypted using the low-trust symmetric key K'. The remainder of the message would remain
15 unencrypted. However, those skilled in the art would not receive any indication that the data for generating the leveled key, *i.e.* the data introduced into the leveling function for leveling the low-trust symmetric key, have to be derived from the unencrypted part of the message.

Instead, those skilled in the art would do nothing with the unencrypted
20 part of the message as taught by Nardone. Possibly, the Examiner considers that those skilled in the art would derive the hash data from the encrypted part of the message of Nardone and would not derive this data from the X-fields. This would, however, be completely against the teaching of Van Oorschot because as stated in column 6, lines 60-63, the use of the leveled key makes
25 sure that any terrorists cannot delete the X-fields from a transmission. If those

senders would delete X-fields, then the CIA would have to break a 1024-bits private key, rather than a 512-bits private key. This is much more work and time compared to breaking the low-trust public key. Therefore, any terrorists would, of course, be interested in deleting the X-fields so that only the high level
5 high-trust public key remains in A' header field. However, if those terrorists could delete the X-fields, then the leveling function cannot be calculated anymore in a correct manner so that the leveled key cannot be calculated anymore, and the correct symmetric key K' for performing a symmetric decryption, as stated in Fig. 4, could not be gained anymore.

10 Therefore, those skilled in the art would never receive a teaching from Van Oorschot not to use the X-fields anymore for providing data into the leveling function, because this is the feature of Van Oorschot which makes sure that any party cannot simply remove the X-fields to upgrade the overall security of the communication to a 1024-bits RSA encryption.

15 Now, a further questions is, whether those skilled in the art would, when reading Van Oorschot use data from the non-encrypted portion of the message for calculating te leveling function. If those skilled in the art would do that, then any party who wished simply to upgrade the system could easily delete the X-fields because the leveling function would work anyway because it does not
20 depend on the low-trust public key. Therefore, those skilled in the art could immediately do what is negated in column 6, lines 60-64.

Furthermore, a leveling function would work in this case safely because the encrypted part of the message has bene transmitted to the receiver and the receiver can decrypt using the correct leveling function and by using his own
25 high-trust private key.

However, the CIA would not be in the position anymore to retrieve the low-trust public and to use this public key to calculate the corresponding private key by, for example, an exhaustive search to break the encryption to be able to read an unencrypted message sent by a reader from a low-trust environment, such as a country known for terrorist activities.

To summarize, there are two main reasons why those skilled in the art would not combine Van Oorschot and Nardone in the manner as stated by the Examiner. The first reason is that those sending messages from a low-trust environment are, of course, interested that the full message is encrypted because the encryption is there that any Government Authorities or Law Enforcement Authorities cannot read the content. Van Oorschot is not directed to any movies, but is directed to the transmission of secrets, which have to be secret before any Government Authority. Therefore, those skilled in the art would not understand Van Oorschot in that those should only encrypt a part of the message. This would not make any sense because then the Government Authority could already read the unencrypted part of the message without any effort.

The second main reason is that the only protection against an attack, in which the X-fields are simply removed, as stated in column 6, lines 60-64, is that the data in the X-fields are necessary for calculating the leveling function. In this context, it is to be noted that the X-fields must be an encrypted symmetric key K' using a low-trust public key encryption and that, additionally, the low-trust public key of entity A has to be there so that, in case of any extraordinary situation, a Government Authority would be in the position to calculate the corresponding private key to decrypt the encrypted message using a decrypted

low-trust symmetric key. Thus, if one would introduce data into the leveling function from the unencrypted part of the message, the safeguard for the X-fields, which allows the Government to break the encryption of the message would be avoided which would be against the complete teaching of Van Oorschot for those skilled in the art.

The Examiner on page 3, line 14, says that the unencrypted second section of the payload data is processed. Here, the Examiner compares the term "payload data" of Claim 1 to the X-fields, which are, of course, not any message component, but which are a 512-bits RSA public key of A and K' RSA-encrypted under this key, as stated in column 7, lines 6 and 7. However, as stated in Claim 1, the second section includes audio data, video data, a combination of audio data and video data, text data, or binary data forming an executive program. In Van Oorschot, the X-fields definitely do not include any payload data. X-fields are not at all allowed to include any payload data, as defined for breaking an encryption, which is the encrypted symmetric key, and the public key used for encrypting the symmetric key. This is acknowledged on page 4, lines 1, 2 and 3 of the Office Action.

However, the conclusion at page 4, lines 8-12 is erroneous. Even when those skilled in the art would only partly encrypt the message in Van Oorschot, then those skilled in the art would not receive any indication that the leveling function has to be calculated from the unencrypted portion of the message. Instead, those skilled in the art would still calculate the leveling function using the X-fields.

Therefore, a straight-forward combination of Nardone to Van Oorschot would not mean that the unencrypted part of the message is used for calculating the leveling function.

As stated before, this would make the Van Oorschot system useless
5 because then any attackers can simply delete the X-fields to upgrade the overall security of the communication to 1025-bits RSA encryption, which would result in substantially increasing the difficulties for the CIA for example to break the encryption.

Therefore, even who those skilled in the art would combine Van
10 Oorschot and Nardone they would not arrive at the inventive device, in which the authenticity of the unencrypted second part is protected by using this data for deducing information and for linking said information and said payload data key to obtain the basic value which is then encrypted.

From this aspect, it also becomes clear that Van Oorschot and Nardone
15 are not at all interested in authenticity. Nardone simply says to not encrypt the whole data and does not care about the unencrypted part, assuming that the authenticity of the unencrypted part is not touched, while Van Oorschot provides a full-encrypting system useful for being cryptographically attached by a Government Authority.

20 Claims 8, 11-12, 18 and 20-21 are rejected under 35 U.S.C. § 103(a) as being obvious in a light of a hypothetical three way combination of Van Oorschot, Nardone and Matyas. Applicant respectfully traverses this rejection. Claims 8 and 11-12 depend upon claim 1, discussed above, and should thus be patentable for at least the same reasons. Claims 18 and 20-21 depend upon
25 claim 17, discussed above, and should thus be patentable for at least the same

reasons. Furthermore, as there is no motivation to combine Van Oorschot and Nardone for the reasons discussed above, by extension there can be no motivation to combine Van Oorschot, Nardone *and* Matyas, as such a three way combination would involve an unmotivated combination of Van Oorschot
5 and Nardone.

Claim 9 is rejected under 35 U.S.C. § 103(a) as being obvious in a light of a hypothetical four way combination of Van Oorschot, Nardone, Matyas and Klemba. Applicant respectfully traverses this rejection. Claim 9 depends upon claim 1, discussed above, and should thus be patentable for at least the same
10 reasons. Furthermore, as there is no motivation to combine Van Oorschot and Nardone for the reasons discussed above, by extension there can be no motivation to combine Van Oorschot, Nardone Matyas *and* Klemba, as such a four way combination would involve an unmotivated combination of Van Oorschot and Nardone.

15 Claim 10 is rejected under 35 U.S.C. § 103(a) as being obvious in a light of a hypothetical four way combination of Van Oorschot, Nardone, Matyas and Edenson. Applicant respectfully traverses this rejection. Claim 10 depends upon claim 1, discussed above, and should thus be patentable for at least the same reasons. Furthermore, as there is no motivation to combine Van
20 Oorschot and Nardone for the reasons discussed above, by extension there can be no motivation to combine Van Oorschot, Nardone Matyas *and* Edenson, as such a four way combination would involve an unmotivated combination of Van Oorschot and Nardone.

Claim 13 is rejected under 35 U.S.C. § 103(a) as being obvious in a light
25 of a hypothetical four way combination of Van Oorschot, Nardone, Matyas and

Schneier. Applicant respectfully traverses this rejection. Claim 9 depends upon claim 1, discussed above, and should thus be patentable for at least the same reasons. Furthermore, as there is no motivation to combine Van Oorschot and Nardone for the reasons discussed above, by extension there can be no
5 motivation to combine Van Oorschot, Nardone Matyas *and* Schneier, as such a four way combination would involve an unmotivated combination of Van Oorschot and Nardone.

Claim 15 is rejected under 35 U.S.C. § 103(a) as being obvious in a light of a hypothetical three way combination of Van Oorschot, Nardone and
10 Roedigar. Applicant respectfully traverses this rejection. Claim 9 depends upon claim 1, discussed above, and should thus be patentable for at least the same reasons. Furthermore, as there is no motivation to combine Van Oorschot and Nardone for the reasons discussed above, by extension there can be no motivation to combine Van Oorschot, Nardone *and* Roedigar, as
15 such a three way combination would involve an unmotivated combination of Van Oorschot and Nardone.

Claim 22 is rejected under 35 U.S.C. § 103(a) as being obvious in a light of a hypothetical three way combination of Van Oorschot, Nardone and Schneier. Applicant respectfully traverses this rejection. Claim 22 depends
20 upon claim 17, discussed above, and should thus be patentable for at least the same reasons. Furthermore, as there is no motivation to combine Van Oorschot and Nardone for the reasons discussed above, by extension there can be no motivation to combine Van Oorschot, Nardone *and* Schneier, as such a three way combination would involve an unmotivated combination of
25 Van Oorschot and Nardone.

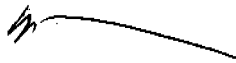
Claim 30 is rejected under 35 U.S.C. § 103(a) as being obvious in a light of a hypothetical three way combination of Van Oorschot, Nardone and Kane. Applicant respectfully traverses this rejection. Claim 30 depends upon claim 17, discussed above, and should thus be patentable for at least the same reasons.

5 Furthermore, as there is no motivation to combine Van Oorschot and Nardone for the reasons discussed above, by extension there can be no motivation to combine Van Oorschot, Nardone *and* Kane, as such a three way combination would involve an unmotivated combination of Van Oorschot and Nardone.

Applicant respectfully posits that all of the claims are allowable over the
10 cited art of record. Should the Examiner deem it helpful, he is encouraged to contact's Applicant's attorney, Michal A. Glenn at (650) 474-8400.

Respectfully submitted,

15



Michael A. Glenn

Reg. No. 30,176

20 Customer No. 22,862